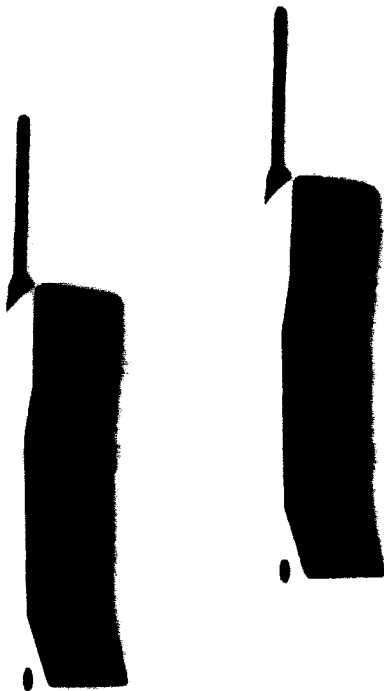


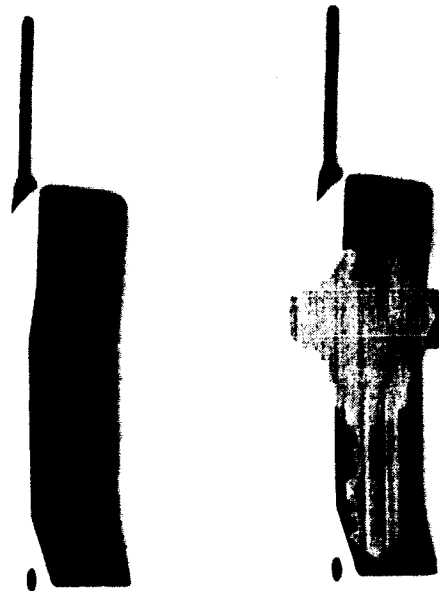
Eras of Cellular Telephony

Antiquity



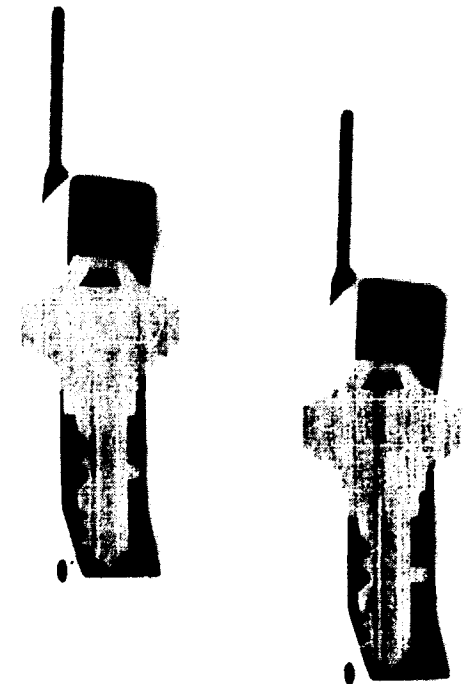
1983-1995
Identification

Sticky



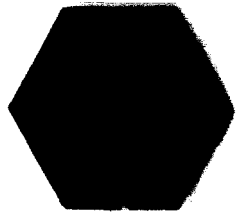
1995-200?
Hybrid
Identification and
Authentication

Ubiquity

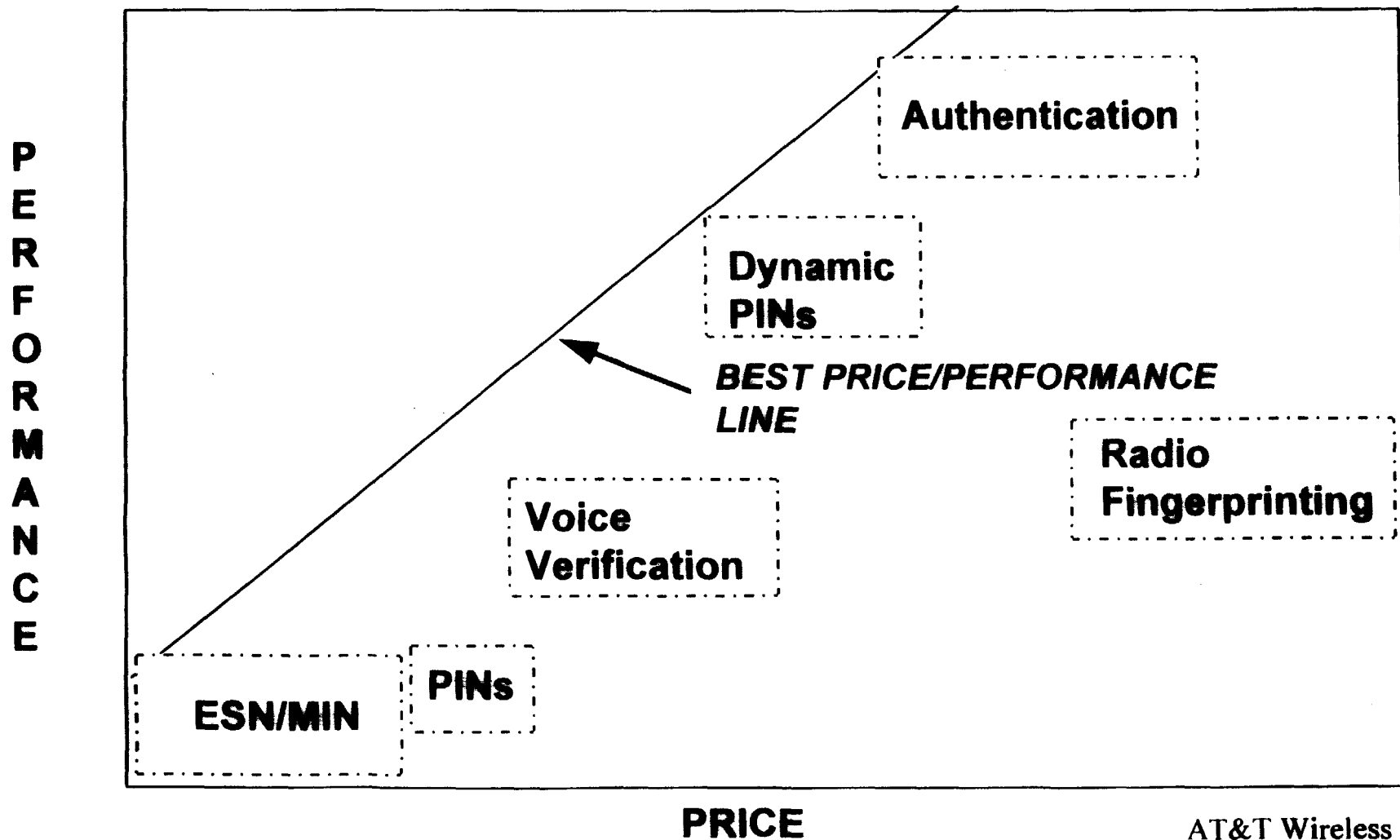


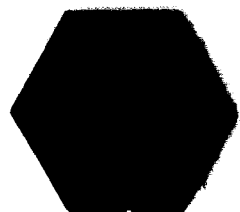
200?-20??
Authentication

AT&T Wireless Services

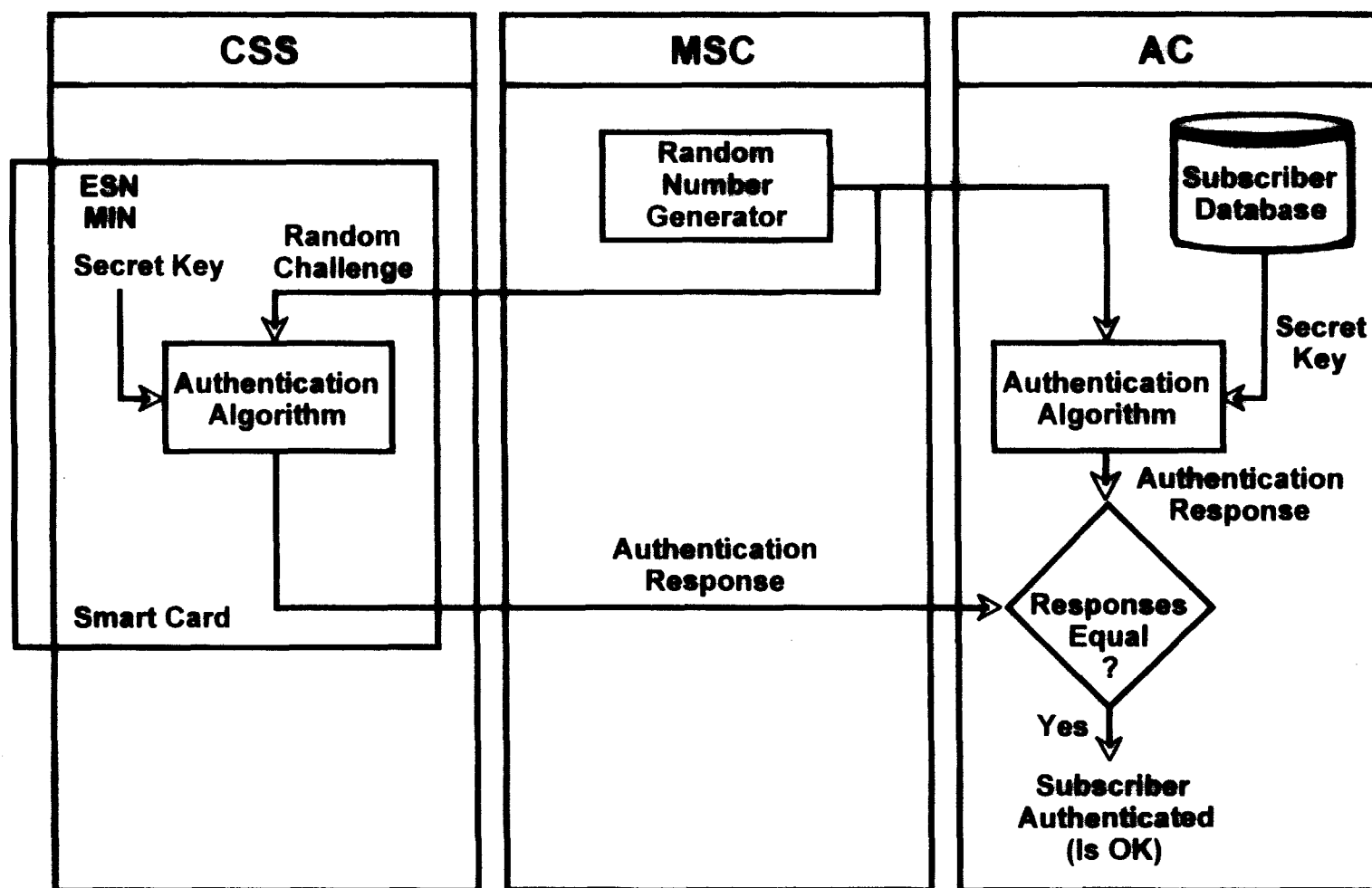


Fraud Solutions Price-Performance

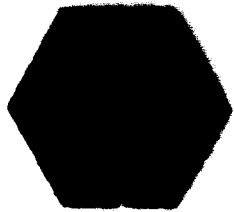




Authentication Scheme with Smart Card – GSM/PCS



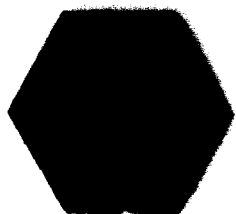
700-47



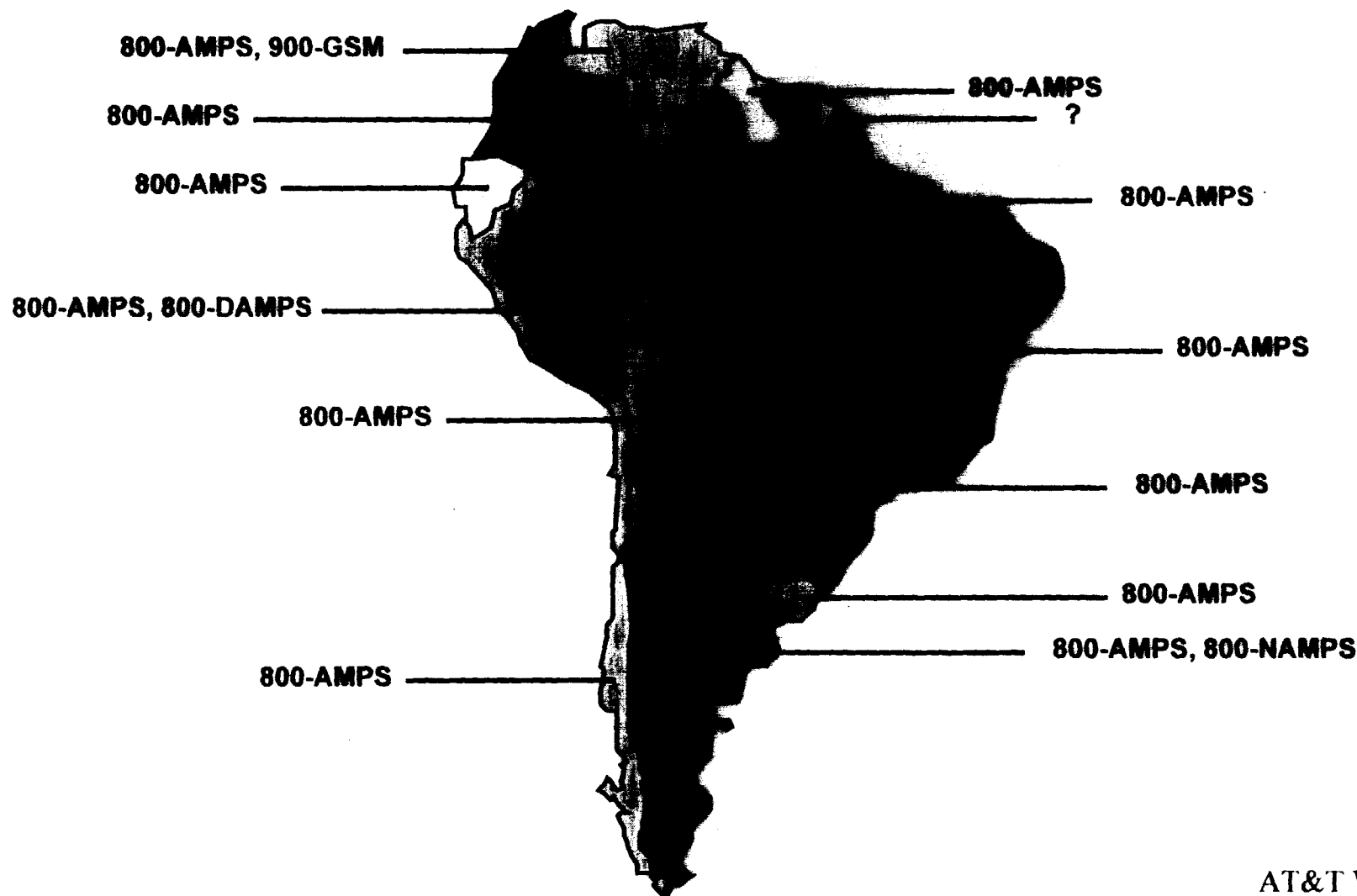
South American Countries



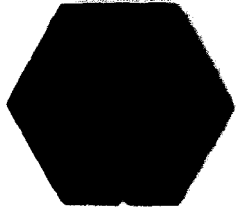
Cellular Fraud: History, Status, Technology, and Prevention



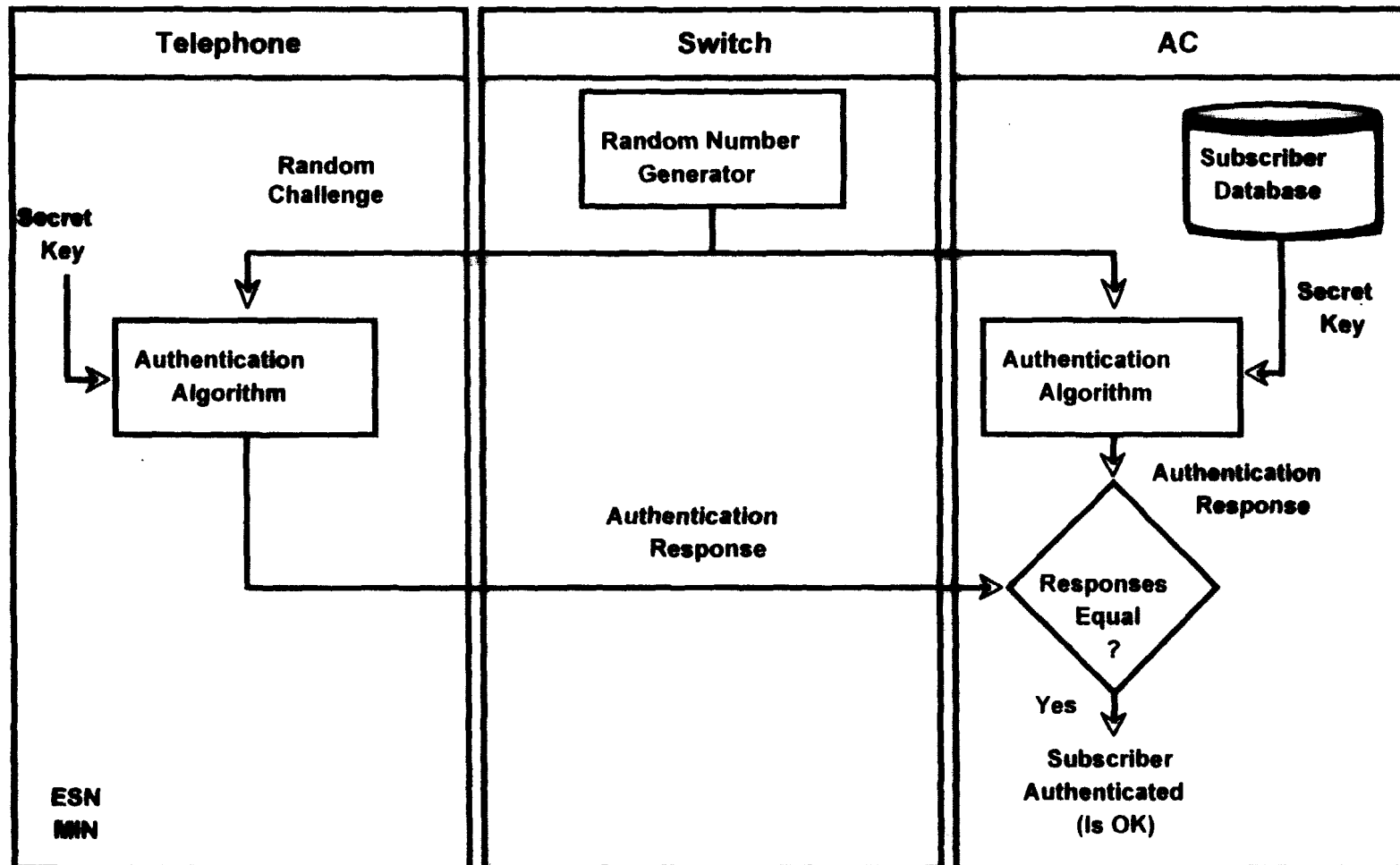
South American Countries Cellular Implementations



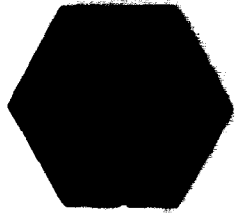
AT&T Wireless Services



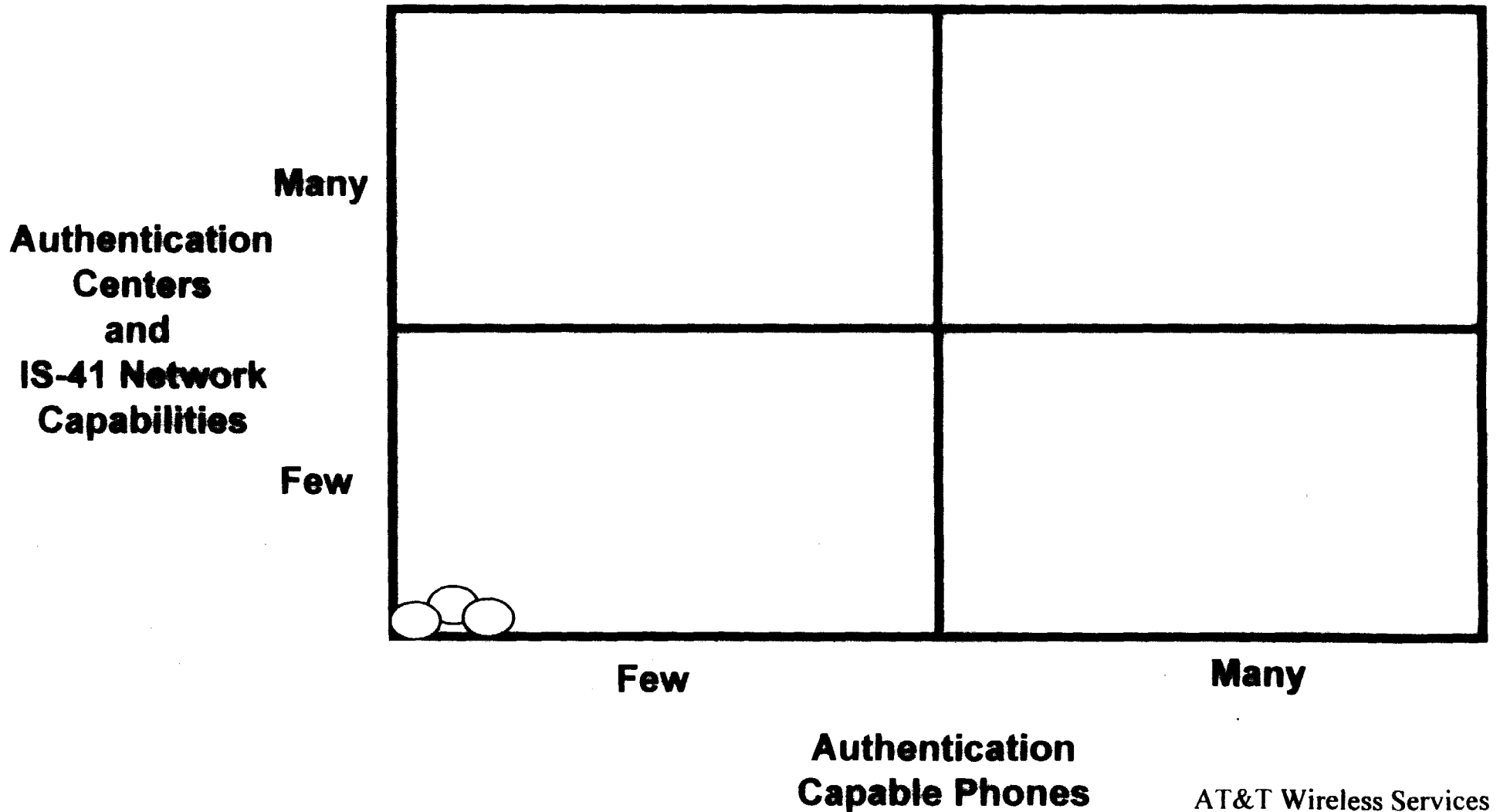
Principle of Cellular Authentication

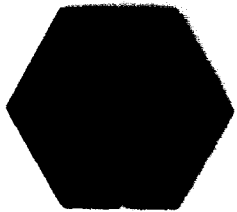


700-63

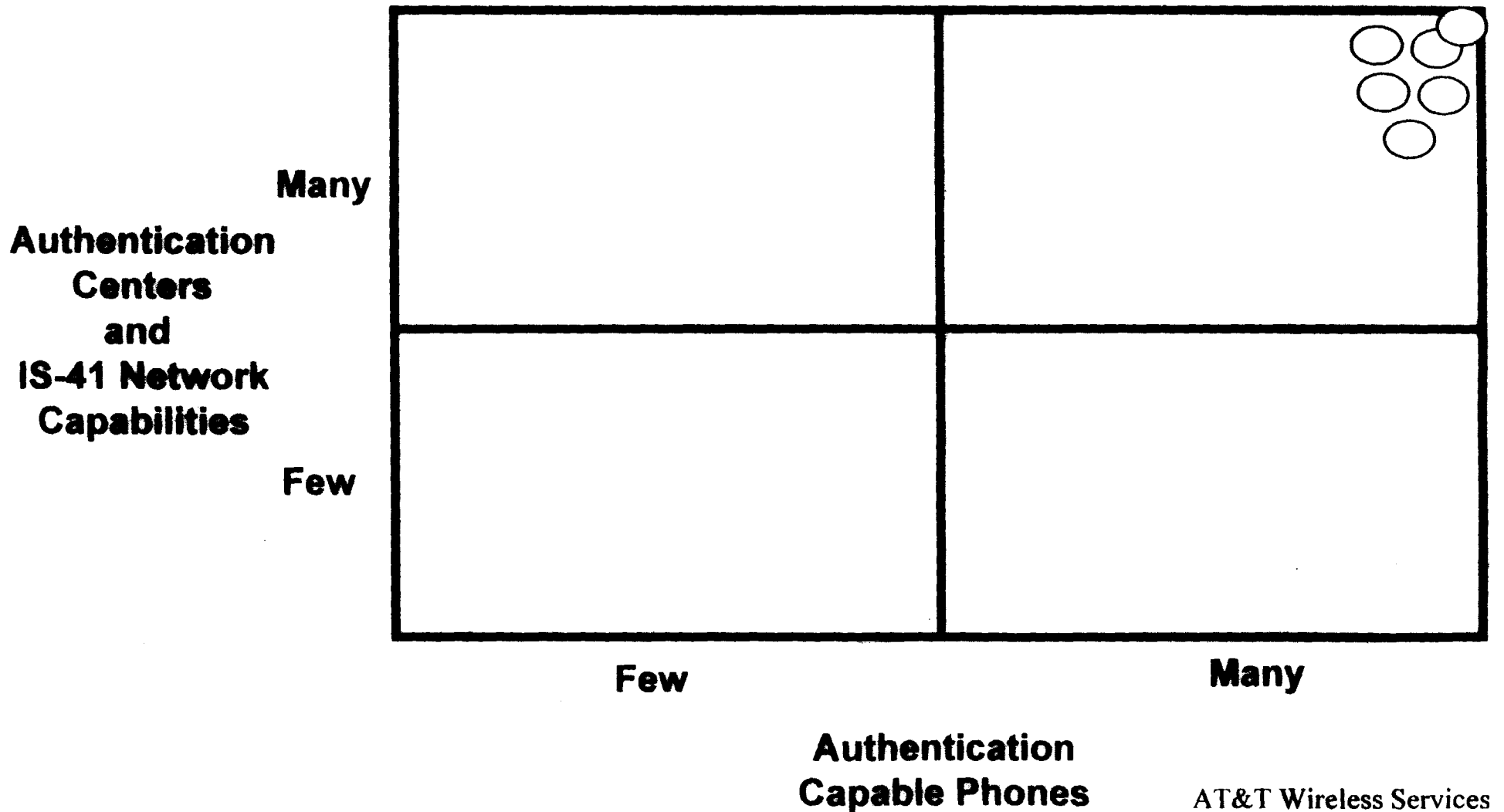


Industry Authentication Effectiveness Map – 1995

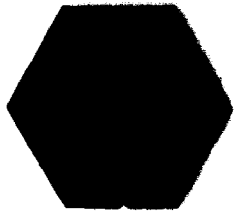




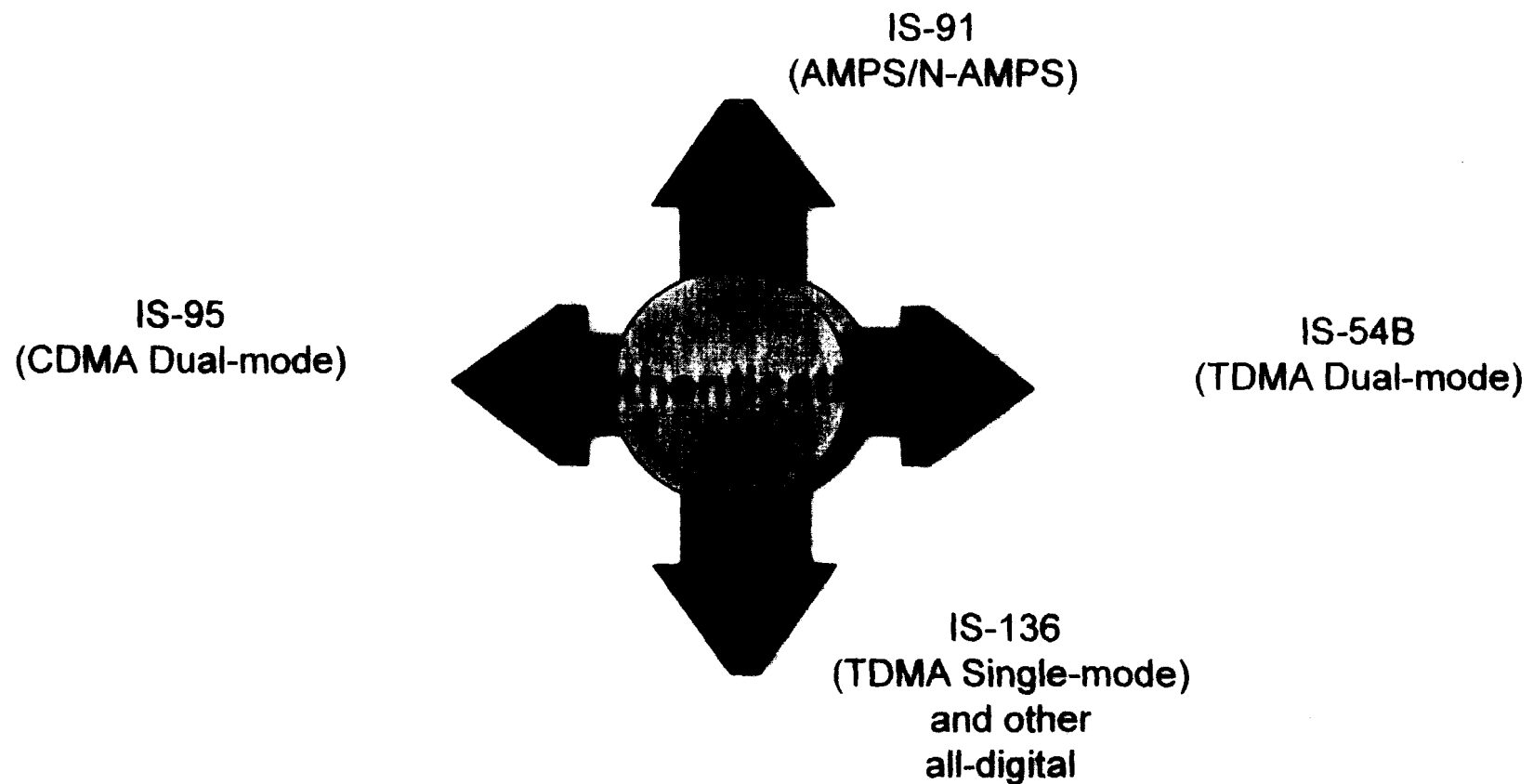
Industry Authentication Effectiveness Map - The Future



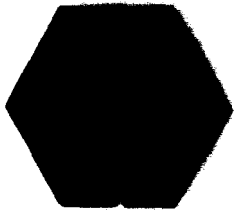
Cellular Fraud: History, Status, Technology, and Prevention



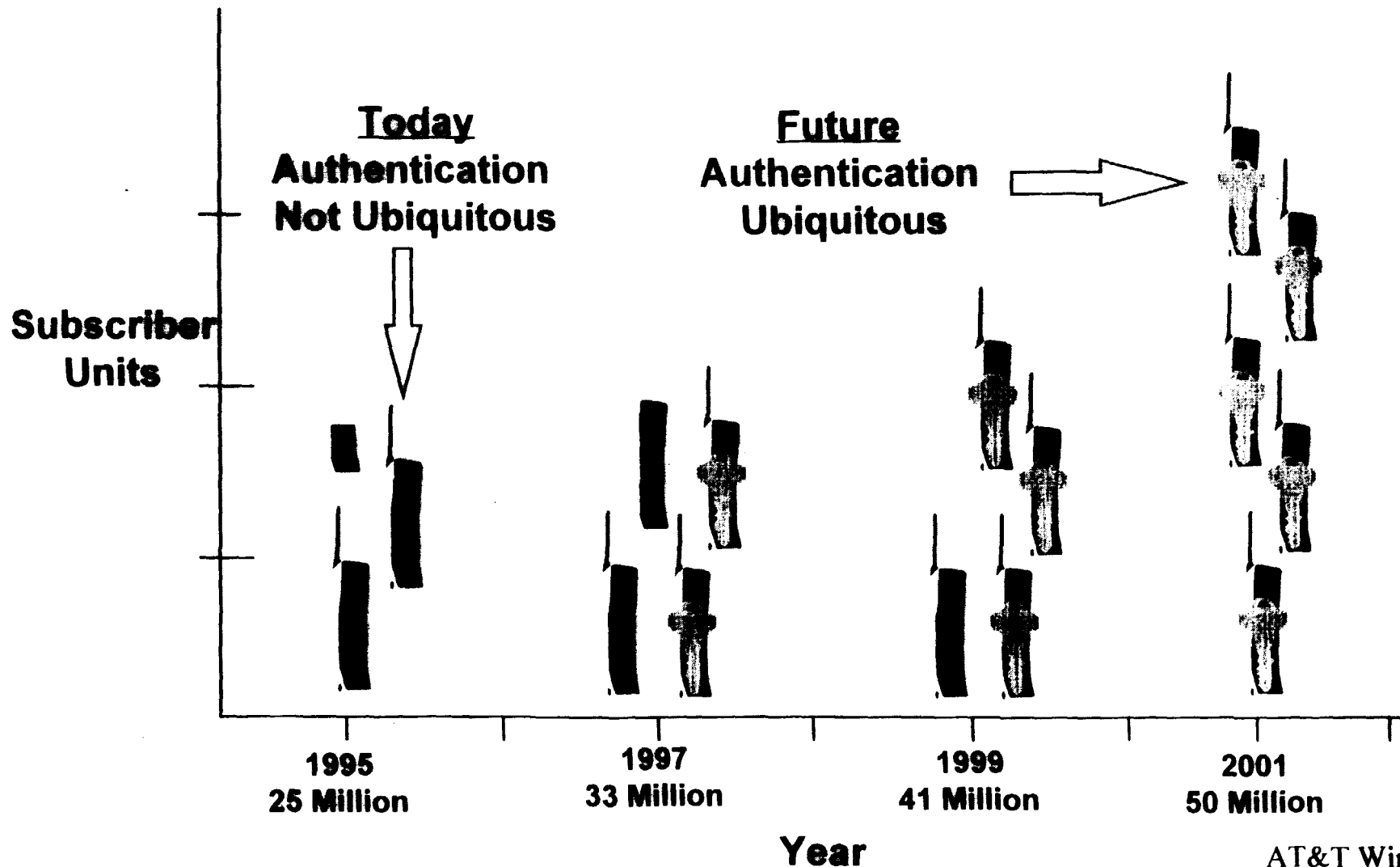
Authentication Alternatives for Cellular Telephones

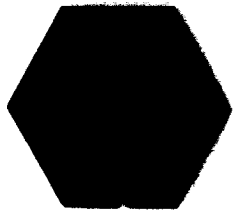


AT&T Wireless Services



Transitioning to Authentication Capable Telephones – A Strategy



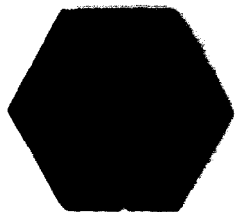


Winning the Battle



***Cryptographic
Authentication***

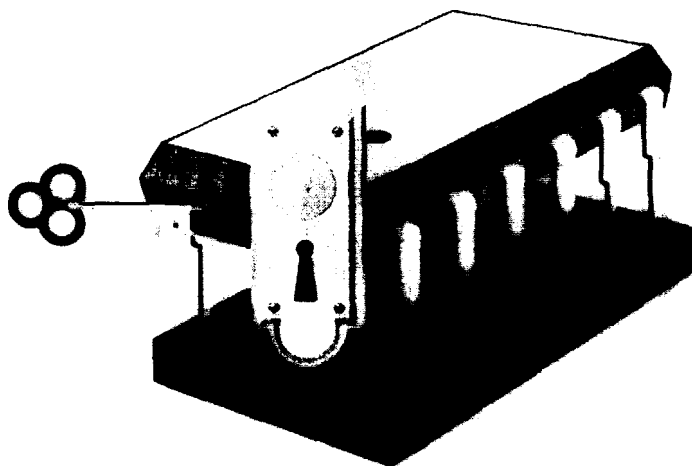
***Enhanced
Network
Security***



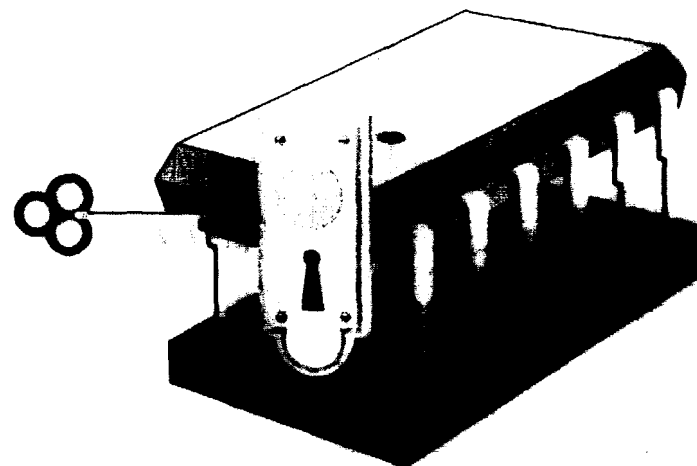
Cellular Fraud: History, Status, Technology, and Prevention

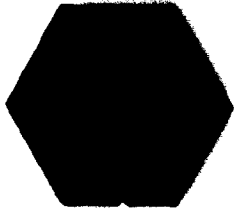
Technical Efforts to Enhance Telephone Security

ESN Storage

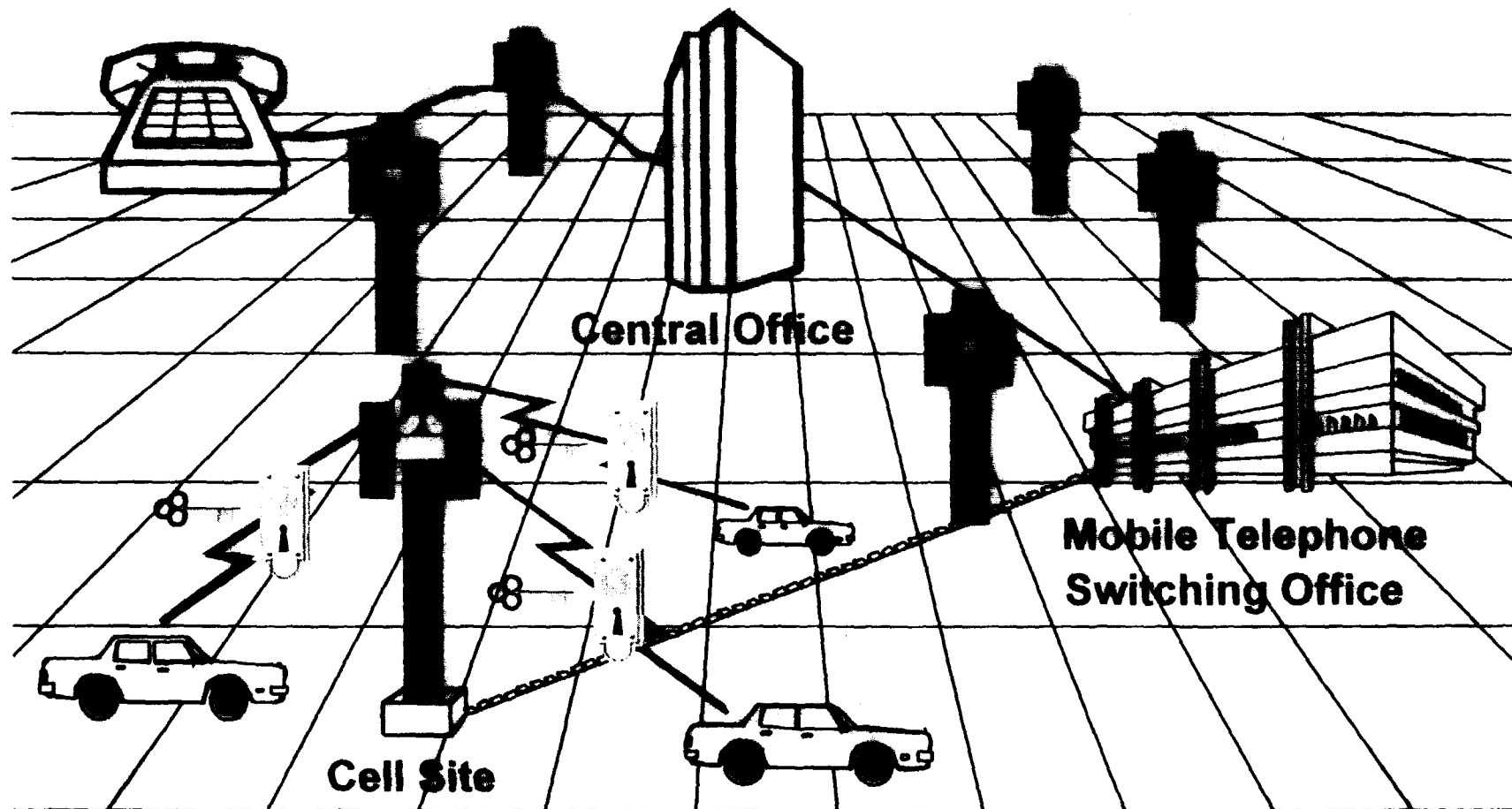


Firmware Storage

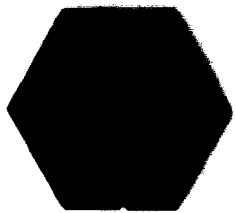




Cellular Fraud Control – Locking the Radio Path

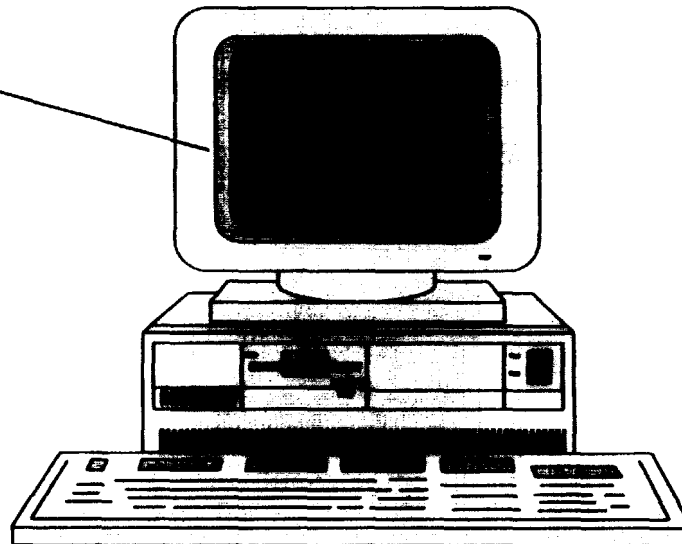


700-3

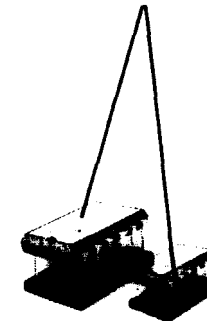


Typical Class B Counterfeiting

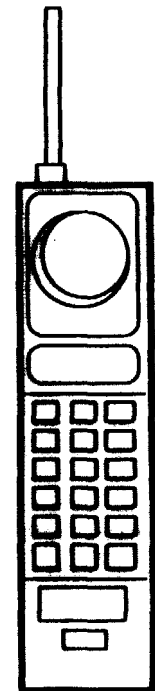
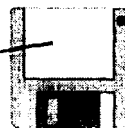
IBM-Compatible PC

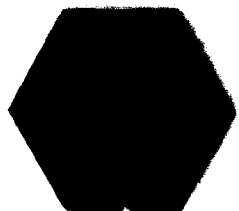


PROM or serial
EEPROM Chips



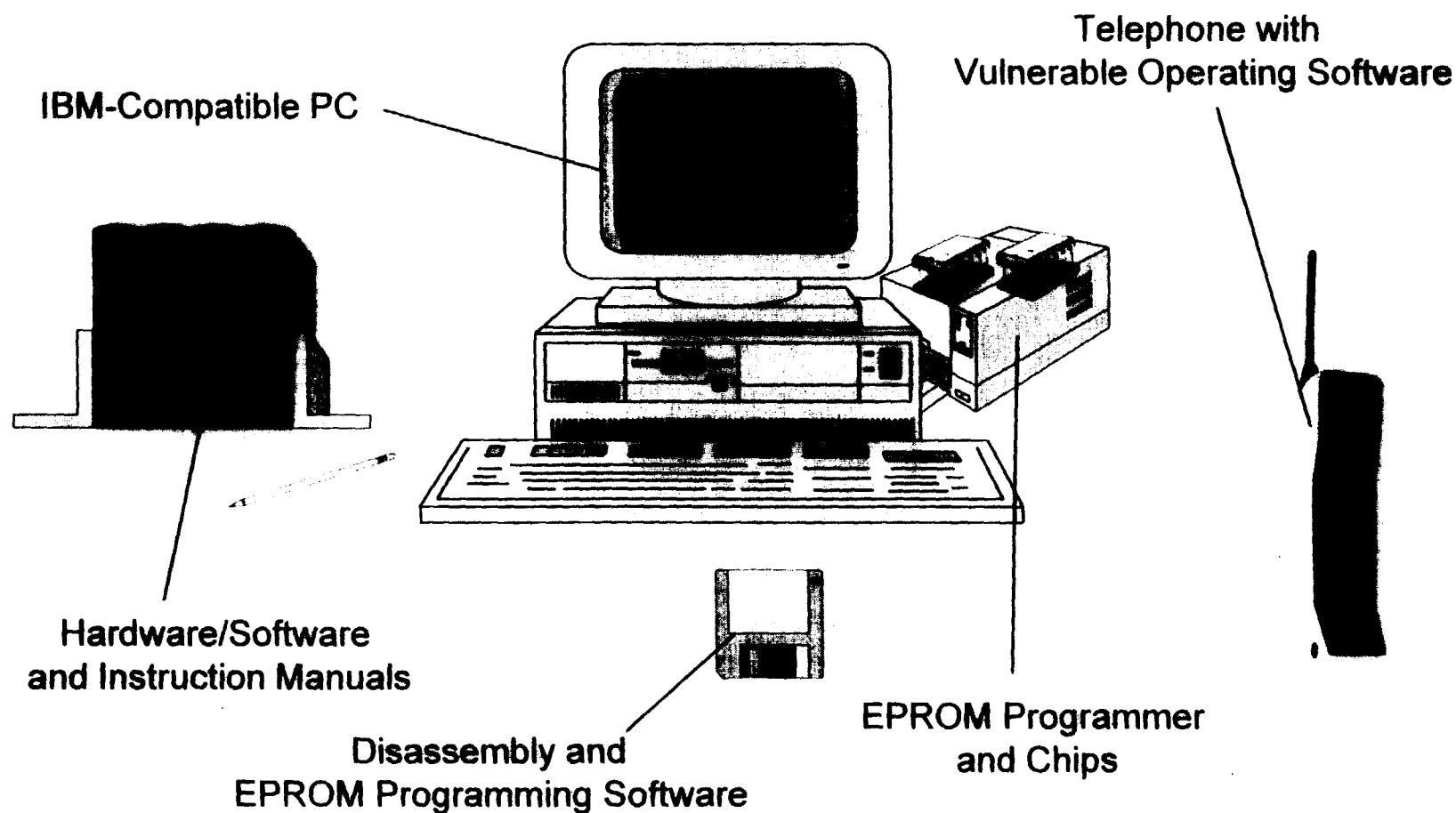
Counterfeiting Software
or EEPROM Programmer



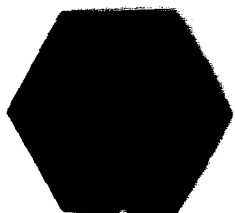


Cellular Fraud: History, Status, Technology, and Prevention

Typical Class C Counterfeiting

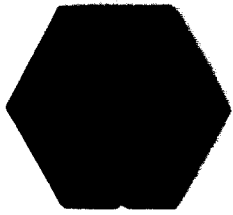


AT&T Wireless Services



Definition of Fraud

- ◆ **The unauthorized and/or illegal use of a cellular telephone or a cellular network. This includes loss of airtime and toll revenues due to misrepresentations by employees, customers, and criminals.**



Cellular Fraud in North America

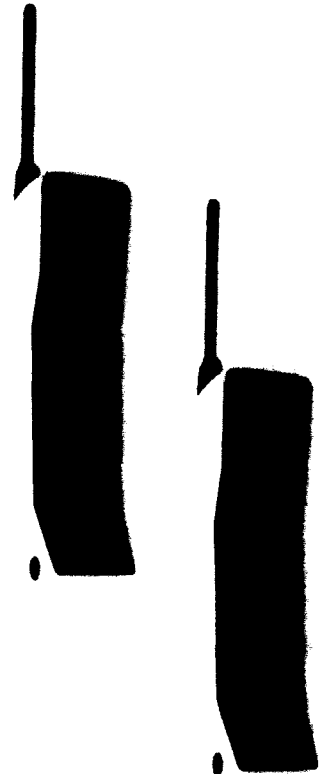
Cellular Communications Era (1983-??)

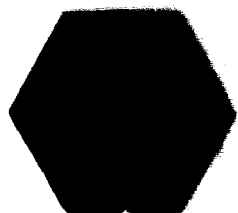
| | |
|--|------------------------------|
| Roamer Fraud Period (1985-1988) | 204,000 Subscribers |
| | 2 Million Subscribers |

| | |
|--|--------------------------------|
| Tumbling Fraud Period (1989-1992) | 2.7 Million Subscribers |
| | 11 Million Subscribers |

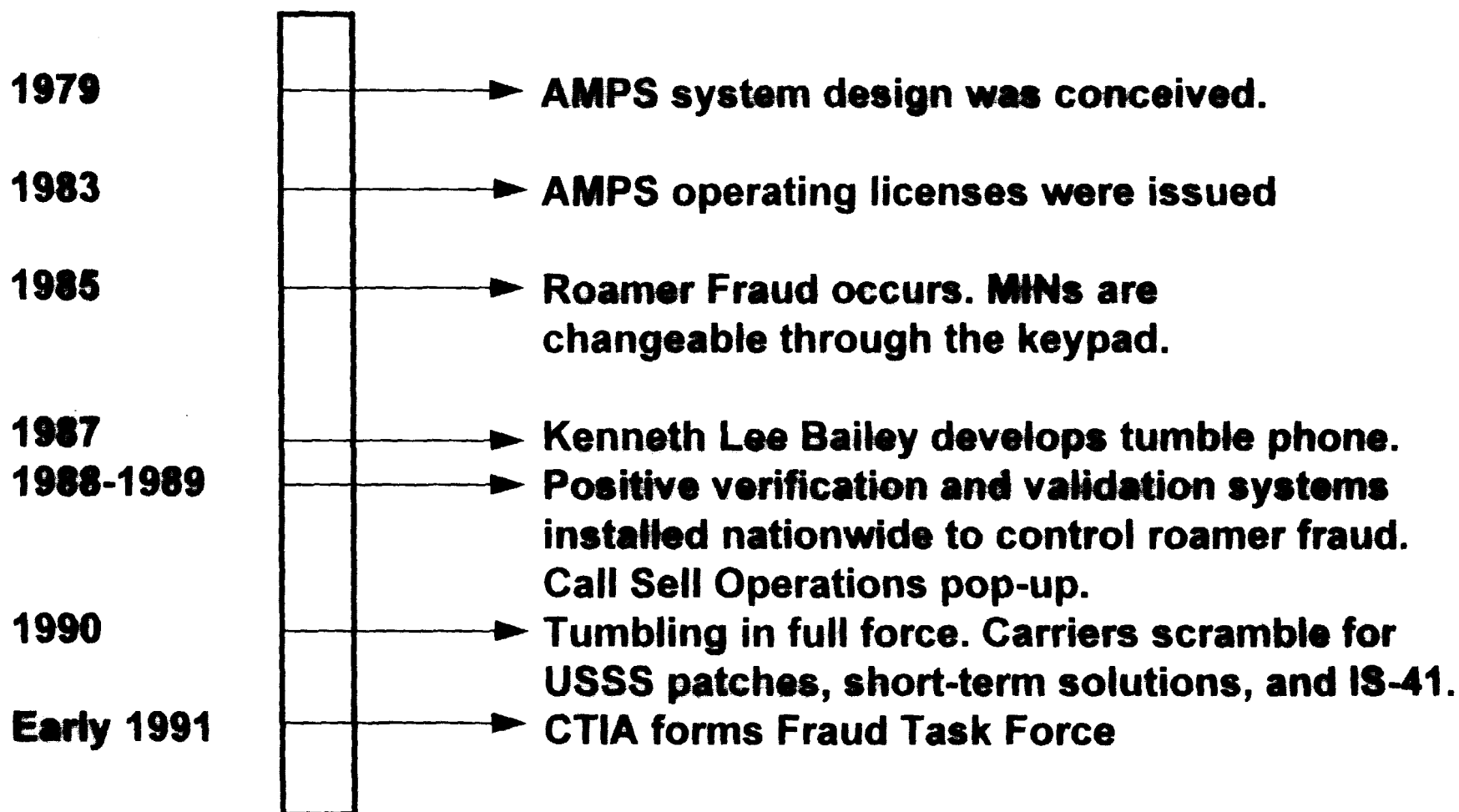
| |
|---|
| Cloning Fraud Period (1992-200?) |
|---|

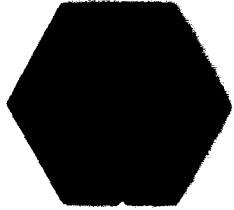
1996: 33 Million Subscribers





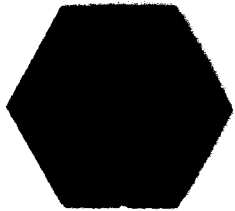
History of Cellular Fraud in North America





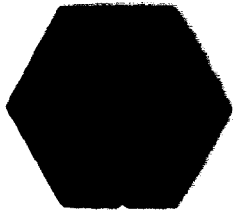
History of Cellular Fraud in North America (continued)

- | | | |
|-------------------|---|---|
| Early 1991 | → | Anthony Timson software enters the marketplace. |
| 1991 | → | Pre-call validation prevents tumbling. |
| 1992 | → | Cloning begins. ESN Readers are used as a tool to capture ESN/MIN pairs. IS-54B specification finalized. |
| Mid-1993 | → | CTIA forms Technical Analysis Laboratory |
| Early 1994 | → | Taiwanese Black Boxes appear. Lifetime telephones by Clinton Watson appear. |
| 1994 | → | New forms of Timson software and systems appear. Second generation lifetime appears. |
| Early 1995 | → | CopyCat Boxes appear widely. PINs are used. |
| Mid-1995 | → | All types of counterfeiting systems are prevalent. |
| Early 1996 | → | Authentication begins. |



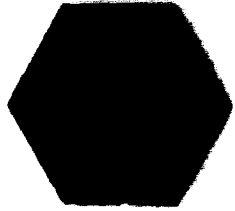
Facts Regarding Cellular Fraud

- ◆ **Fraud will never go away completely**
- ◆ **Typically associated with other criminal activities (gambling, racketeering, drug dealing, etc.)**
- ◆ **Existing antifraud tools will ultimately have minimal impact**
- ◆ **Heightened awareness will work for/against problem**
- ◆ **Weakness of single link may compromise whole system**

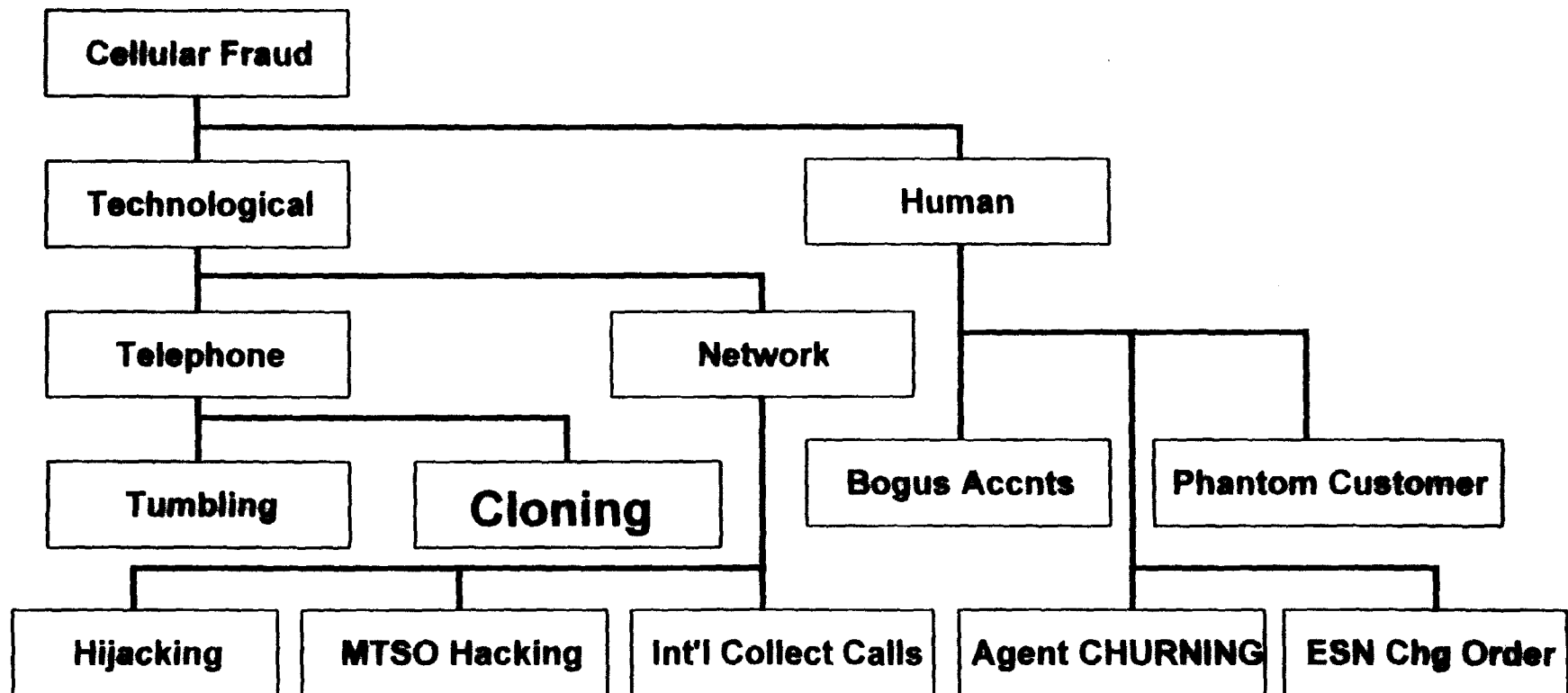


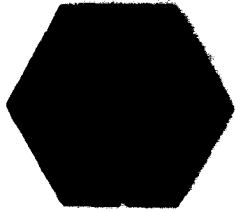
More Disturbing Cellular Fraud Trends

- ◆ **Fraud will get significantly worse in the near term**
- ◆ **“Honest” people are committing fraud**
- ◆ **Cellular bandits have plenty of money and resources**
- ◆ **“Cellphone phreaking” concepts are shared**
- ◆ **Bandits are getting more technically sophisticated**
- ◆ **Software “tools” are becoming more readily available with Information Superhighway access**

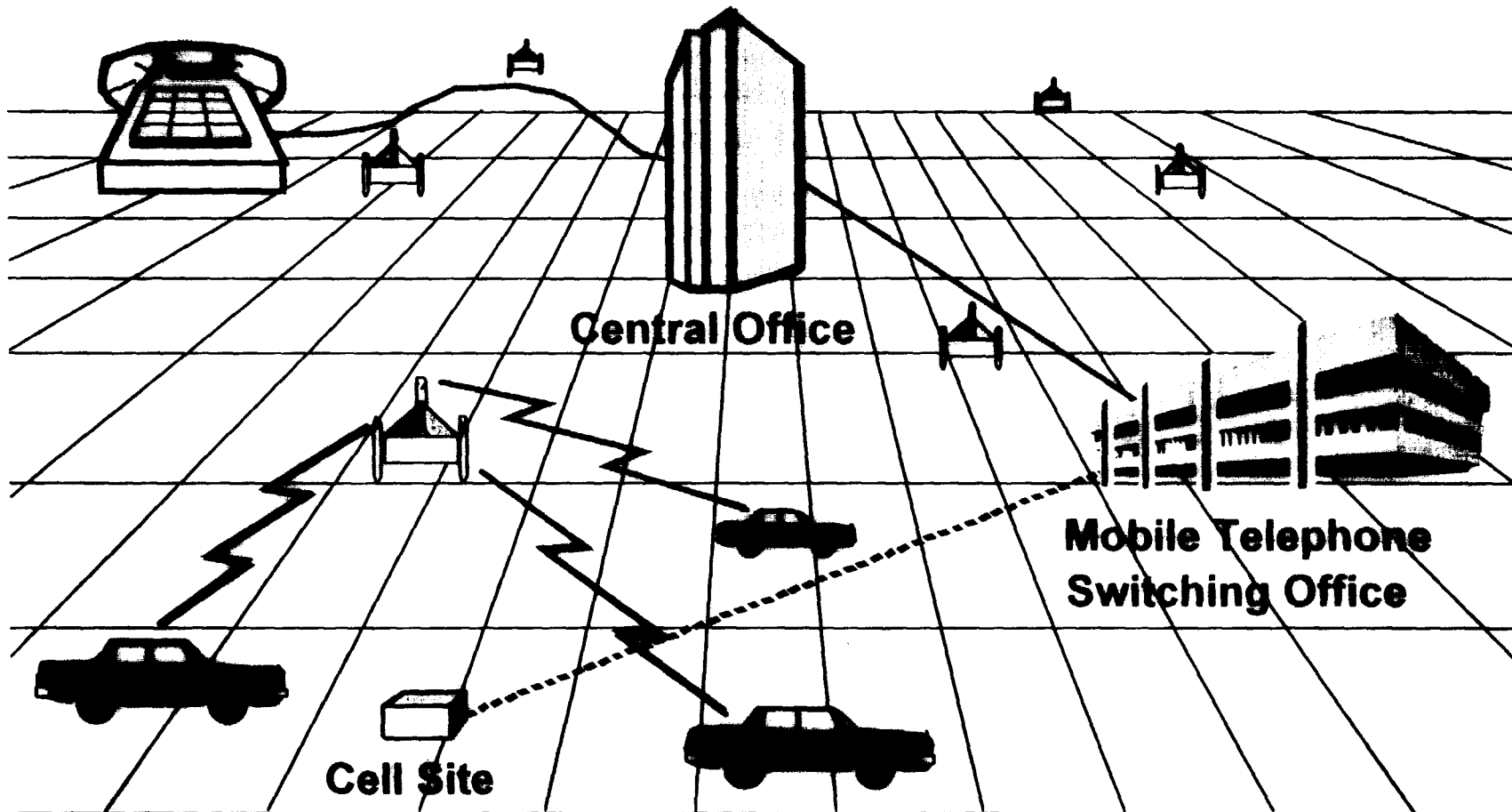


General Taxonomy of Cellular Fraud

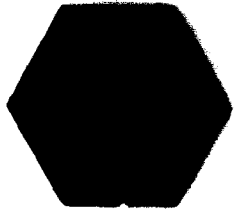




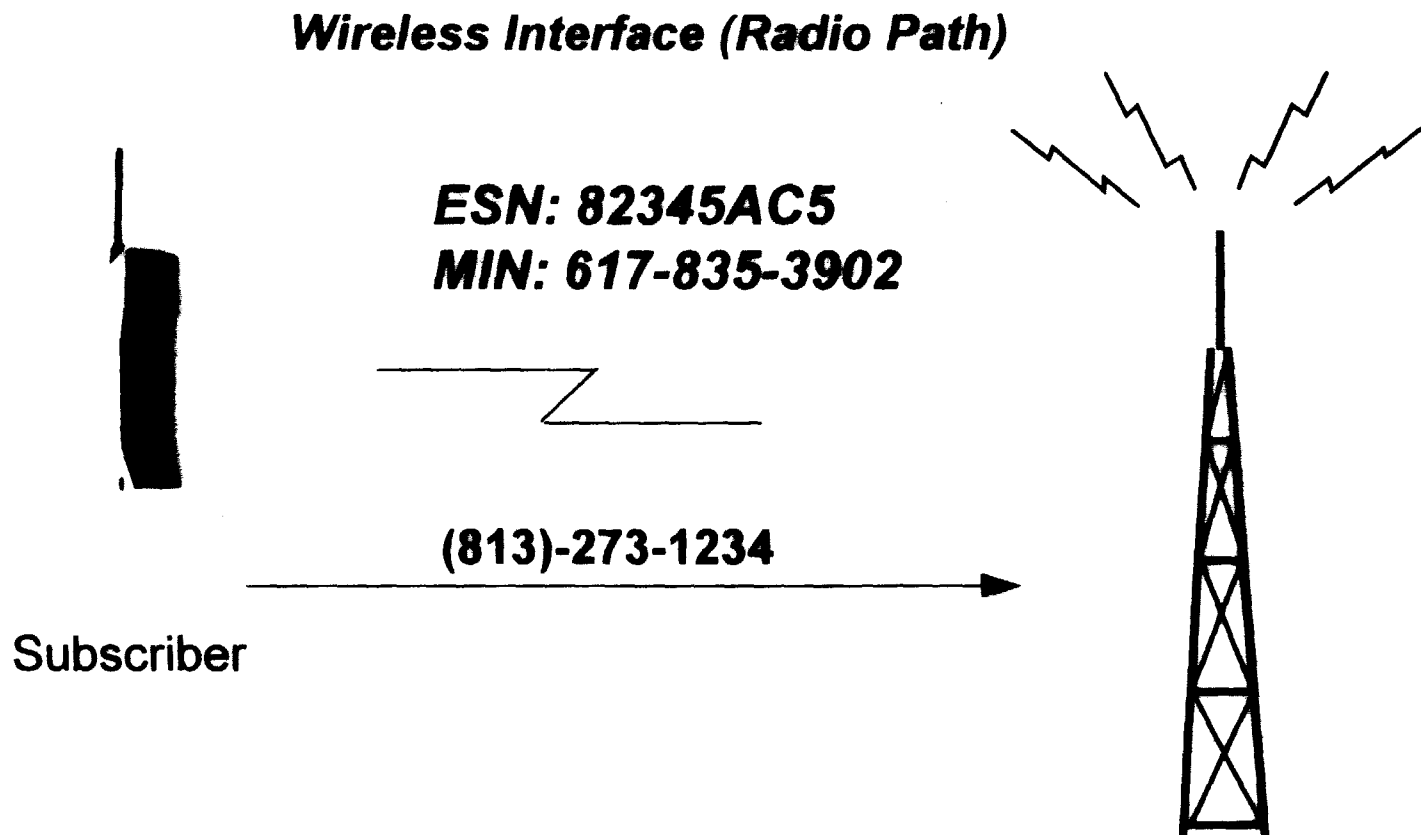
Principle of Cellular Telephony



700-3



Typical Cellular Call – No validation



Cloning: The Approach

